Press release
13-02-2024 - 09:46
20240212IPR17618

European Parliament

Artificial Intelligence Act: committees confirm landmark agreement

- Safeguards agreed on general purpose artificial intelligence
- Limitation for the of use biometric identification systems by law enforcement
- Bans on social scoring and AI used to manipulate or exploit user vulnerabilities
- Right of consumers to launch complaints and obtain meaningful explanations

MEPs have endorsed at committee level the provisional agreement on the Artificial Intelligence Act that ensures safety and complies with fundamental rights.

On Tuesday, the Internal Market and Civil Liberties Committees voted 71-8 (7 abstentions) to approve the result of negotiations with the member states on the Artificial Intelligence Act.

This regulation aims to protect fundamental rights, democracy, the rule of law and environmental sustainability from high-risk AI. At the same time, it aims to boost innovation and establishing Europe as a leader in the AI field. The rules put in place obligations for AI based on its potential risks and level of impact.

Banned applications

The agreement bans certain AI applications that threaten citizens' rights, including biometric categorisation systems based on sensitive characteristics, untargeted scraping of facial images from the internet or CCTV footage for facial recognition databases, emotion recognition in

Press Service, Directorate General for Communication
European Parliament - Spokesperson: Jaume Duch Guillot
Press switchboard number (32-2) 28 33000

workplace and schools, social scoring, predictive policing based solely on profiling a person or assessing their characteristics, and AI that manipulates human behaviour or exploits people's vulnerabilities.

Law enforcement exemptions

The use of biometric identification systems (RBI) by law enforcement is prohibited in principle, except in exhaustively listed and narrowly defined situations. "Real-time" RBI can be deployed only under strict safeguards, e.g. limited in time and geographic scope, with prior judicial or administrative authorisation. Such uses involve, for example, searching for a missing person or preventing a terrorist attack. Using such systems after the fact ("post-remote RBI"), which is considered high-risk, also requires judicial authorisation, and has to be linked to a criminal offence.

Obligations for high-risk systems

Clear obligations were also agreed for other high-risk AI systems, which could significantly impact health, safety, fundamental rights, environment, democracy and the rule of law. High-risk uses include those in critical infrastructure, education and vocational training, employment, essential services (e.g healthcare, banking), certain systems in law enforcement, migration and border management, justice and democratic processes (e.g. influencing elections). Citizens will have a right to launch complaints about AI systems and receive explanations about decisions based on high-risk AI systems affecting their rights.

Transparency requirements

General-purpose AI (GPAI) systems, and the models they are based on, have to meet certain transparency requirements and comply with EU copyright law during their training. More powerful GPAI models that could pose systemic risks will face additional requirements, including performing model evaluation, risk assessment and reporting on incidents. Additionally, artificial or manipulated image, audio or video content ("deepfakes") needs to be clearly labelled as such.

Measures to support innovation and SMEs

Regulatory sandboxes and real-world testing will be established at national level, offering SMEs and start-ups opportunities to develop and train innovative AI before placement on the market.

Next steps

The text awaits a formal adoption in an upcoming Parliament plenary session and final Council endorsement. It will be fully applicable 24 months after entry into force, except bans on prohibited practises, which will apply 6 months after the entry into force; codes of practise (nine months after entry into force); general-purpose AI rules including governance (12 months after entry into force); and obligations for high-risk systems (36 months).

Further information

Text of the agreement on the AI Act
Procedure file
Profile of the rapporteur Brando Benifei (S&D, Italy)
Profile of the rapporteur Dragos Tudorache (Renew, Romania)
Committee on the Internal Market and Consumer Protection
Committee on Civil Liberties, Justice and Home Affairs

Contacts

Yasmina YAKIMOVA
Press Officer
(+32) 2 28 42626 (BXL)
(+32) 470 88 10 60
yasmina.yakimova@europarl.europa.eu
imco-press@europarl.europa.eu
@EP_SingleMarket

Janne OJAMO
Press Officer
(+32) 2 284 12 50 (BXL)
(+32) 470 89 21 92
janne.ojamo@europarl.europa.eu
libe-press@europarl.europa.eu
@EP_Justice